EXHIBIT N

Arete Advisors

October 13, 2017

William Dugan, Esq.
Baker & McKenzie LLP
452 Fifth Avenue
New York, NY 10018

**Re: *KCG Holdings, Inc. and KCG Americas, LLC v. Rohit Khandekar*, SDNY No. 17-cv-3533**

Dear Mr. Dugan:

I have been retained by Plaintiffs KCG Holdings, Inc. and KCG Americas, LLC (collectively, "KCG") in the above-referenced matter to analyze Rohit Khandekar's creation and use of custom computer programs known as "scripts" and other operations he performed in KCG's systems environment, and to provide an opinion as to whether Khandekar accessed KCG confidential information without proper authorization. My analysis and opinions are set forth below.

## I. Executive Summary

I have reached the following conclusions based on my academic training in computer science, my experience in the computer and digital forensics industry, and my review and analysis of certain pleadings and evidence in this matter (as set forth in Section III):

- Khandekar's access, copying and reviewing of confidential source code files he obtained from other users' directories constitutes a security breach and unauthorized access under KCG policy.

- Khandekar deliberately circumvented the security controls and mechanisms put in place by KCG to protect its source code files and other confidential and proprietary information.

- Khandekar developed at least seven scripts to search other users' folders and directories for [redacted] computer programs and to capture the permission levels associated with each file, to specifically identify unencrypted source code files.

- Between December 28, 2016 and March 28, 2017, Khandekar ran the scripts he created on multiple occasions against other users' folders and directories and performed numerous operations in other user's folders and directories, such as viewing, copying, filtering and deleting files.

- Khandekar targeted and acquired [redacted] source code files developed by other users, which he was not authorized to access, copy or review.

- Khandekar took explicit actions to destroy evidence of his actions by deleting files and folders that stored KCG confidential and proprietary information retrieved by his scripts and wiping certain devices.

I provide my opinions in this matter with a reasonable degree of professional certainty, based on the information available to me at this time. I understand that discovery is ongoing, and I reserve the right to amend or supplement my opinions as appropriate if more information is provided.

## II. Expert Qualifications

I have over 30 years of technical and managerial experience in systems, software development, security engineering, digital forensics, and electronic discovery. I am currently the Chief Operating Officer at Arete Advisors, Inc. Arete Advisors is a Cyber Security firm that focuses on data-centric investigations. Prior to Arete, I was the Chief Technology Officer at Discovia where I co-lead the Digital Forensics practice and function as a technology subject matter expert. Prior to Discovia, I was a Vice President a Celerity Consulting, Inc., where I lead the Digital Forensics and Technology Integration Practices. Prior to Celerity, I was a Director at Deloitte FAS, LLP, where I was the National Practice Leader for Discovery Services.

Over the past several years I have served as a presenter, panel speaker, instructor, and roundtable representative at several industry conferences and seminars in the United States, Canada, and Europe on numerous information technology and security related topics. In addition, I have authored over 25 articles and technical papers on information security, computer forensics, electronic discovery, records management and other related topics in such publications as Internet Security Advisor, Data Communications, Information Security, DM Review, COTS Journal, Lotus Advisor, and the Metropolitan Corporate Council.

I hold a doctorate degree in Computer Science from Colorado Technical University, a graduate degree in Computer Data Management from Webster University and an undergraduate degree in Technical Management and Computer Science from Regis College. I hold two technology-related patents regarding message-based software architecture and an enterprise security process. I am recognized by the National Computer Security Center as a Vendor Security Analyst ("VSA") and have been certified by the ISC2 as a Certified Information System Security Professional ("CISSP"), certificate number 4140.

My recent engagements include the following types of matters (1) software intellectual property theft relating to algorithms used within high-frequency trading, (2) an email fraud case, (3) an evaluation of software development approach and schedule in a software development contract dispute, (4) an evaluation of software development process issues, (5) a software IP dispute, (6) a comparative software analysis related to a software licensing dispute, and (6) an evaluation of the security controls of a computer system to determine if they were adequate to protect Company Confidential information. A copy of my curriculum vitae is attached hereto as **Exhibit A**. I am being compensated in this matter at a rate of $750.00 per hour.

## III. Materials Reviewed

I reviewed and analyzed the following data and information produced by the parties in this matter upon which I based my opinions:

1. KCG Server Directory Trees
2. GNU/Linux System Bash Command History
3. Emacs Files
4. List of [redacted] Source Codes with Additional PGP Recipients
5. Khandekar Scripts
6. Emails Produced by the Parties in Discovery
7. Relevant Pleadings
8. Khandekar Employment Agreement and Employment Policies
9. KCG Information Security Policies
10. KCG Secret Code-Related Policies
11. Transcript of October 5, 2017 Deposition of Rohit Khandekar

## IV. Factual Background

KCG is a financial services firm that engages in proprietary algorithmic trading and electronic market making. Am. Comp. at ¶ 10.[1] In April 2012, a KCG predecessor entity hired Khandekar as a Quantitative Strategist. *Id.* at ¶ 15. As part of KCG's customer market making signal team, Khandekar was responsible for developing and refining predictive models that use information to forecast price movements in securities markets ("Predictors"). *Id.* at ¶¶ 25, 26; Khandekar Tr. at 45.

KCG Predictors are highly confidential and often contain secret source code developed by Quantitative Strategists. Am. Comp. at ¶ 25, 26; Khandekar Tr. at 57-59. Khandekar testified at his deposition that the way a Predictor responds to certain information or events, what values the Predictor computes, and how the Predictor computes those values can all be considered confidential. Khandekar Tr. at 57-59. He also acknowledged that Quantitative Strategists were not allowed to know the confidential parts of Predictors (referred to internally as the "secret sauce") that they did not develop. *Id.* at ¶ 89. Khandekar testified that he worked on approximately [redacted] of KCG's predictors and that KCG intentionally walled him off from knowing the secret sauce of the other [redacted]. *Id.* at ¶ 131.

KCG employs various security policy and procedures to ensure Quantitative Strategists do not access the secret source code of Predictors they do not work on. *See* Section V.G., below. Among those is the requirement that Quantitative Strategists encrypt completed (also known

[1] The Amended Complaint for Injunctive and Other Relief, filed August 6, 2017 is referred to herein as the "Amended Complaint" or "Am. Compl."

as "committed") secret source code and enter the code into the SVN, KCG's source code repository. (KCG000440). The encrypted code must contain a list of "Additional PGP Recipients" who are authorized to access the file and may work on a copy of the file in their personal directories on KCG's servers. (KCG000444).

In March 2017, Khandekar accepted a job with Two Sigma, a KCG competitor, where he would be in charge of the signal team. Khandekar Tr. 113. He ended his employment with KCG on March 30, 2017. *Id.* at 281.

In April 2017, shortly after Khandekar's resignation, KCG discovered that Khandekar's personal directory on its server had [redacted] source code files that did not identify Khandekar has an Additional PGP Recipient. (KCG007963; KCG010634). These source code files had been developed by other Quantitative Strategists, not Khandekar. (KCG010634).

In this action, Khandekar has admitted, among other things, that he obtained the [redacted] source code files by (1) writing custom scripts to search other users' directories for unencrypted source code, and (2) copying unencrypted source code files from other users' directories to his own. Khandekar Tr. at 205; Def. Am. Answer at ¶36, 37, 149. Khandekar, however, claims that certain employees whose directories he surreptitiously accessed, copied and reviewed secret source code files from authorized him to do so by "setting the file and directory access permissions on KCG's computer systems accordingly." Def.'s Response to Plaintiff's Interrog. No. 10.

## V. Methodology and Analysis

To render an opinion regarding Khandekar's access and use of KCG's confidential and proprietary information, I designed a protocol that included:

- Analyzing the functionality of the scripts written by Khandekar;
- Reviewing commands Khandekar executed in KCG's systems to identify actions related to his access, copying and reviewing of other users' directories and his deletion of files from his own directory;
- Reviewing data from a text editor program (Emacs) to determine whether Khandekar opened files for which he was not an Additional PGP Recipient;
- Analyzing Khandekar's directory trees to determine if/when the [redacted] source code files at issue were in Khandekar's directories and whether Khandekar was listed as an Additional PGP Recipient for those files;
- Analyzing the plausibility of Khandekar's testimony regarding the wiping of his Samsung Galaxy phone and his KCG-issued laptop; and
- Reviewing KCG's information security and confidentiality policies to determine whether Khandekar's actions violated any of those requirements.

My analysis of each of these issues is discussed in detail below.

### A. Khandekar Scripts

I reviewed and analyzed seven Bash scripts[2] written by Khandekar (the "Khandekar Scripts") to determine their functionality. See Table 1, Khandekar Scripts.

| Name | Bates Number |
|---|---|
| Scan.sh | KCG010655 |
| Process.sh | KCG010656 |
| Scan2.sh | KCG010657 |
| Process2.sh | KCG010658 |
| Scan3.sh | KCG010659 |
| Process3.sh | KCG010660 |
| Scan3a.sh | KCG010661 |

**Table 1– Khandekar Scripts**

I received the Khandekar Scripts in .pdf format. I performed an Optical Character Recognition (OCR) process using Adobe Acrobat software against each .pdf file to covert the file from image to text. I then manually reviewed the converted file against the .pdf version to ensure the conversion was accurate.

In order to determine the functionality of the Khandekar Scripts, I analyzed the code contained in the files in two ways. First, I performed a manual analysis of each script and documented the functionality of each line of code to understand the behavior of each line of code during execution. *See* **Exhibit B**, Analysis of Khandekar Scripts. Second, I executed the Khandekar Scripts in a Linux-based virtual machine, which I created in order to replicate the KCG Linux environment. I evaluated the behavior of the Khandekar Scripts in the Linux-based virtual machine and confirmed the results were consistent with my manual analysis. *See id.*

Based on my analysis, the Khandekar Scripts can be grouped in two categories: Scan Scripts (Scan.sh, Scan2.sh, Scan3.sh, Scan3a.sh) and Process Scripts (Process.sh, Process2.sh, Process3.sh). The Scan Scripts search user directories to locate [redacted] computer files and capture the permissions (read/write/execute) associated with each file, which reveals whether the file is unencrypted. *See* **Exhibit B**. The Process Scripts read and display the names and contents of the files identified by Scan Scripts to enable Khandekar to filter the files. *See id.*

### B. Bash History Log Files

I reviewed and analyzed Khandekar's Bash (command line) history between 2016-11-07 15:47:06 UTC – 2017-28-03 19:11:37 UTC, which was approximately 15,000 unique lines of

[2] Bash is the shell, or command language interpreter, that allows a user to interact with the GNU/Linux operating system on which KCG's build server runs. The user can type a specific Bash command to cause an action, such as copying or deleting a file. A Bash script is a sequence of commands that can be saved and executed repeatedly.

command long.[3] To identify commands that might be indicative of Khandekar searching for or copying secret source code developed by other users, I formulated a protocol to search Khandekar's Bash history for specific actions. I sought to identify instances where Khandekar was executing the Khandekar Scripts, moving from his own directory to other employees' directories, searching for [redacted] files, viewing file contents, and copying those files to his own directory, or removing directories. Using a software tool, dtSearch, I searched for specific Bash commands such as "cd" (changing directories), "cp" (copying files), and "rm" (removing files), and reviewed those command lines as well as the surrounding command lines for related actions.

I compiled the results of my search in a detailed timeline of Khandekar's Bash command operations, attached as **Exhibit C**. As part of this process, I located and converted the Unix timestamps, which are captured in the Bash history log files, into a Coordinated Universal Time (UTC) date and time.

My review of the Bash history revealed that, between December 28, 2016 and March 28, 2017, Khandekar executed the Scan and Process Scripts and performed various operations on files and folders residing in other users' directories and took steps to delete evidence of his conduct. Specifically, Khandekar performed the following operations to search, view and copy files from other users' directories to his own directory and to remove evidence of his actions:

- Executing the Khandekar Scrips against other users' directories;
- Viewing content, word count, line count and file size information for files in other users' directories;
- Comparing file contents to view the differences between files in other users' directories;
- Copying files from other users' directories to hidden folders in his own directory;
- Hiding the folder in which he stored other users' source code files so that it would not appear in response to standard searches;
- Displaying information about other users;
- Moving source code files copied from other users' directories into a subfolder labeled "done;"
- Copying/cloning an entire Git source code repository existing in [redacted] user directory ; and
- Deleting files and folders from his own directories containing files he copied from other users' directories.

## C. Emacs Data

I reviewed Emacs files[4] that were generated when Khandekar opened certain [redacted] source code files and automatically saved by the Linux system. The goal was to determine whether

[3] The Bash history was provided in .pdf format. I converted the .pdf files to searchable text by performing an OCR process with the Adobe Acrobat software.

[4] Emacs is a text editor program used in this context for viewing and writing source code. The Emacs files were produced in .pdf format. (KCG010595-KCG010633).

Khandekar opened source code files for which he was not listed as an Additional PGP Recipient that were identified in his directory as of February 19, 2017, and to review the available evidence of Khandekar opening source code files while using the Emacs text editor.[5] To that end, I first reviewed a list of [redacted] source code files that Khandekar read using Emacs. (KCG010605). Next, I identified the Emacs auto-save files associated with each source code file on the list. I then reviewed the Emacs auto-save files associated with each source code file. Finally, I reviewed the list of [redacted] source code files to determine whether Khandekar was listed as an "Additional PGP Recipient" of the source code files with which each Emacs file was associated. (KCG0010634).

Based on my review, I determined that Khandekar used Emacs to open at least [redacted] source code files for which he was not an "Additional PGP Recipient." He opened some of these files on multiple occasions, primarily throughout the month of January 2017. For example, he opened source code files [redacted] multiple times on January 9-10, 2017, and [redacted] multiple times on January 12, 13 and 14, 2017. (KCG010605).

### D. Source Codes

To determine whether Khandekar's personal directories contained source code files for which he was not an Additional PGP Recipient, I reviewed a list of [redacted] source code files (KCG010634) and a .pdf of Khanderkar's build server directory tree (KCG007963), which was taken from a February 19, 2017 snapshot of the server, and a screenshot of Khandekar's build server directory structure as it existed in the February 19, 2017 snapshot. (KCG000061).

Among other identifying metadata, the source code list contains [redacted] source code files, and for each file, identifies the authorized PGP recipients by username. Khandekar's username, rkhandek, is not listed as an "Additional PGP Recipient" of any of the source code files on the list. I then reviewed the February 19, 2017 snapshot of Khandekar's build server directory tree to determine whether any of the [redacted] source code files were saved in his directory on the date of the snapshot. My review confirmed that each of the [redacted] source code files were present in Khandekar's build server directory on February 19, 2017.

I also reviewed Khandekar's organization of source code files into subfolders within his directory tree as of February 19, 2017. The snapshot reveals that, within his build server folder, the source codes files are organized into various subfolders, including the subfolder "done." As seen in the Bash History, Khandekar deliberately moved certain source code files into this folder after reviewing them.

[5] Emacs does not necessarily record all files opened in Emacs, and thus, the information available is likely incomplete. Because Emacs is a text editor program, the Emacs timestamps for a particular file may not correlate with the Bash command timestamps. For example, a user may issue a command to read a file; but if the file is left open on the user's system, the Emacs auto-save may record the timestamp along the continuum of time that the file is open or further interacted with by the user.

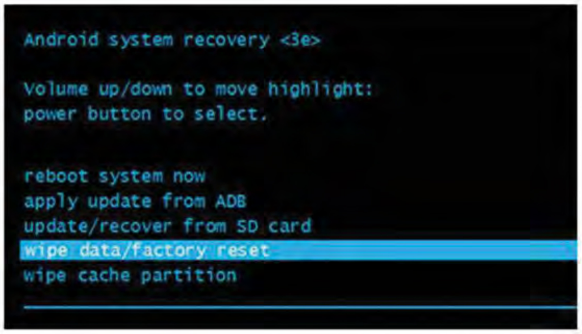
### E. Samsung Phone

I reviewed the portion of Khandekar's deposition testimony in which he explained how he wiped his personal Samsung Galaxy S6 Phone on March 20, 2017. According to Khandekar's testimony, the following occurred:

(i) The phone was fully charged;
(ii) The phone suddenly switched off;
(iii) He tried to turn the phone on but it did not work;
(iv) He went online and found instructions, which told him to press three buttons simultaneously to turn the phone on in a "particular mode" and to select the second option;
(v) He pressed three buttons;
(vi) Before he could get a chance to stop pressing those buttons and select the second option, he accidentally selected the first option; and
(vii) The phone did a factory reset and wiped all of his contacts and information off the phone.

Khandekar Tr. 238-240

To determine whether Khandekar's testimony is consistent with how the Samsung Galaxy S6 operates, I reviewed the Samsung Galaxy S6 User Manual, which addresses how to perform a factory reset if the phone is turned on, but not if the phone is powered off, as Khandekar testified his phone was. I then searched for additional resources and reviewed the following: (i) "Factory Data Reset (Powered Off) - Samsung Galaxy S6 edge +" Troubleshooting Page from Verizon Wireless website; (ii) "Device resets: Samsung Galaxy S 6" from T-Mobile Support Website; and (iii) Galaxy S6: How to Factory Reset, from Android Explained website.[6] These materials demonstrate that, when the recovery screen is shown, the user must navigate down the menu to the factory reset option, as shown in Figure 1 below:

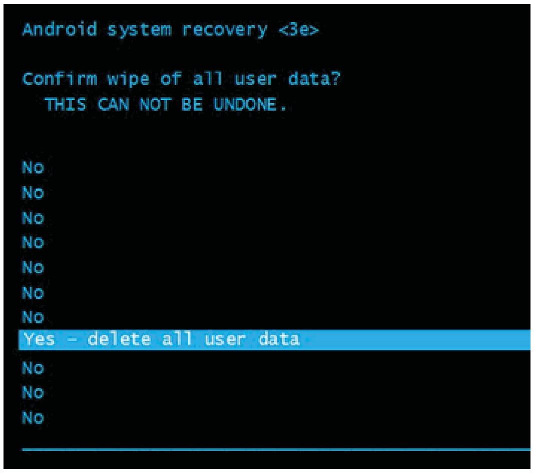


```
Android system recovery <3e>

Volume up/down to move highlight:
power button to select.

reboot system now
apply update from ADB
update/recover from SD card
wipe data/factory reset
wipe cache partition
```

[6] *See* Factory Data Reset (Powered Off) - Samsung Galaxy S6 edge +, available at https://www.verizonwireless.com/support/knowledge-base-174621/, last accessed on Oct. 10, 2017; Device resets: Samsung Galaxy S 6, available at https://support.t-mobile.com/docs/DOC-29296, last accessed Oct. 10, 2017; Galaxy S6: How to Factory Reset, available at https://www.androidexplained.com/galaxy-s6-factory-reset/, last accessed Oct. 10, 2017.

Figure 1 - Samsung S6 Recovery Screen Menu[7]

Further, once the "wipe data/factory reset" option is selected, the user will be directed to second confirmation screen, where they must actively confirm the deletion of all data on the phone, as shown in Figure 2 below:



```
Android system recovery <3e>

Confirm wipe of all user data?
  THIS CAN NOT BE UNDONE.

No
No
No
No
No
No
No
Yes - delete all user data
No
No
No
```

Figure 2 – Samsung S6 Confirmation Screen[8]

My review of these materials is consistent with my own experience with Samsung Galaxy phones. I have performed factory resets in order to reset Samsung Galaxy phones to original factory settings multiple times. The factory reset option, which wipes all of the user data on the device, requires several deliberate steps and a confirmation. My experience is consistent with the images shown above: the phone will display a recovery screen with a list of options; however, factory reset is not the first option, and if factory reset is selected, the user will be required to affirmatively confirm the selection in a second confirmation screen before the phone is wiped.

Based on this information, and my own experience in performing a factory reset on Samsung Galaxy phones, it is my opinion that Khandekar's testimony that he accidentally performed a factory reset of his Samsung Galaxy phone in the manner he described is highly implausible.

### F. KCG-Issued Laptop

I reviewed the portion of Khandekar's deposition testimony regarding his wiping of his KCG-issued laptop. Specifically, he testified that he wiped the laptop before returning it to KCG because he "didn't know of any way" to delete only his personal information while leaving KCG information on the laptop.

[7] Galaxy S6: How to Factory Reset, *supra* at fn. 6

[8] *Id.*

Based on my review of the evidence, Khandekar was a sophisticated computer user who knew how to search for and delete files. This is clearly indicated in the Bash history files that I have reviewed. Khandekar appears to be very familiar with both directory- and file-level operations. Given that he deleted both of these on the KCG servers, I find it highly unlikely that he did not know how to delete files and folders from his KCG-issued laptop. Deleting directories and/or files from a laptop, whether a Windows-based personal computer or an Apple Macintosh-based system, is generally considered a fairly basic operation. I therefore find it highly improbable that Khandekar wiped the computer because he did not know how to selectively delete personal files.

### G. KCG Confidentiality and Security Policies

To provide an opinion regarding whether Khandekar's access, copying and viewing of source code files in other users' directories constitutes "unauthorized access," I reviewed the following KCG policies and agreements addressing the definition, handling, creation, and protection of Company Confidential and Proprietary information:

| Starting Bates No. | Document Title |
|---|---|
| KCG000011 | Employment Agreement |
| KCG000028 | Knight Code of Business Ethics |
| KCG000042 | Confidential Information and Invention Assignment Agreement |
| KCG000045 | KCG Code of Business Ethics |
| KCG000258 | Records Management Policy |
| KCG000266 | Acceptable Use of Encryption Policy |
| KCG000270 | Access Control Policy |
| KCG000286 | Information Management Policy |
| KCG000293 | Information Security Incident Response Policy |
| KCG000299 | Information Security Management Policy |
| KCG000307 | Network Communication Policy |
| KCG000314 | Password Standard Policy |
| KCG000319 | Personal Mobile Device Policy |
| KCG000324 | Physical and Environmental Security Policy |
| KCG000329 | Firm Issued Portable Device Policy |
| KCG000335 | Security Monitoring Policy |
| KCG000340 | System Development Security Policy |
| KCG000424 | Adding new source file - TheLoop - Jul 30 2015 |
| KCG000426 | Committing Secret Code - TheLoop - May 13 2016 |
| KCG000430 | GPG - setting up your environment - TheLoop - Oct 28 2016 |
| KCG000433 | How do I compile a single secret file - TheLoop - May 11 2016 |
| KCG000434 | How does Linux secret code compilation process work_ - ETG Wiki - Feb 17 2012 |
| KCG000440 | How does Linux secret code compilation process work_ - TheLoop - May 12 2016 |
| KCG000444 | New Predictor Release Procedure |
| KCG010691 | Knight - Employee Handbook.pdf |

| | |
|---|---|
| KCG010783 | Acceptable Use Policy |

**Table 3 – KCG Policies and Procedures**

Based on my review, KCG has designed a number of policies and procedures to prevent unauthorized access to information. For example, access to data on KCG's servers is driven by file system permissions that assign rights (*i.e.,* read, write, execute) to specific users or groups. KCG gives employees permissions for only what is needed to perform their job duties. *See* Access Control Policy; *see also* Information Management Policy ("information may be disclosed only to those people who have a legitimate business need for the information…"). KCG also uses "encryption methods to ensure that confidential information cannot be accessed by unauthorized individuals." *See* Encryption Policy.

The Acceptable Use Policy strictly prohibits employees from "[e]ffecting security breaches," which is defined to include "accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access." This policy also prohibits "executing any form of network monitoring which will intercept data not intended for the employee's host…" Further, KCG requires its employees to observe good security practices and keep confidential and proprietary information secure from anyone who does not have a legitimate reason to access the information. *See, e.g.,* Knight Employee Handbook, Confidentiality Policy.

KCG has also developed specific policies and protocols designed to protect confidential source code files and Predictors, including the following:

- KCG maintains a source code repository called the SVN.
- Once a secret source code is completed, the Quantitative Strategist who authored the code encrypts the code and enters it into the secret SVN.
- The author of the secret source code includes in the encrypted code a list of "Additional PGP Recipients" who are authorized to access the secret source code.
- Quantitative Strategists who have such permissions to access a secret source code file may work on it in their personal directories.

I compared the policies and protocols set forth above with the evidence of Khandekar's access to other users' directories and source code files. Based on this analysis, I determined that (1) Khandekar deliberately circumvented KCG's security polices when he wrote scripts to search other users' directories and accessed their source code files; and (2) Khandekar's conduct in this regard constitutes a security breach and unauthorized access of confidential information under KCG policies. The bases for these conclusions are set forth below.

### 1. Khandekar deliberately circumvented KCG policies and procedures designed to protect confidential source codes.

Based on the materials I have reviewed and my 25+ years of experience in the data security industry, it is my opinion that the Khandekar Scripts were designed to circumvent KCG's strict policies governing the treatment of confidential information, specifically source code files.

The Khandekar Scripts provided roadmaps to any unencrypted confidential source code files in user directories. Because KCG required encryption of confidential source code files in the SVN, Khandekar could not view the content of a source code file in the SVN unless he was the author or an Additional PGP Recipient. Thus, Khandekar wrote scripts to search for unencrypted files in other employees' personal directories, and he specifically searched for [redacted] files, which were likely to contain confidential source code. The scripts used a filtering process to remove duplicates and unencrypted source codes that were not confidential.[9] Khandekar then used the results of the scripts to obtain [redacted] source code files that he would not have been able to access through the SVN.

Khandekar took deliberate steps to hide and delete evidence that he had accessed other users' directories and copied their confidential source code files. Specifically, he created a hidden build server folder (".bs") to store the source code files he obtained from other users' directories. In the Unix operating system, a user can create a hidden folder simply using a "." prefix before the name. By naming the folder ".bs" Khandekar hid the folder from the normal directory list command, "ls," which lists all files/folders in a directory.

Khandekar also took a number of steps to delete the source code files and otherwise cover his tracks. Between December 29, 2016 and March 28, 2017, he deleted various directories he created to hold source code files, and on March 6, 2017, he deleted the hidden build server folder, his build server directory and his "docs" directory with recursive force. *See* Section VI; Exhibit C. As discussed above, he also wiped his personal phone, which he also used for KCG business, and his KCG-issued MacBook laptop, in violation of KCG policy, before he resigned. (KCG000329).

Given the restrictions on Khandekar's access to certain source code files, the availability of other avenues to obtain the information he sought (*e.g.,* asking his colleagues), the deliberate design and refinement of the scripts to hone in on confidential source code files that were not encrypted, and Khandekar's deletion of evidence, I conclude with a high degree of professional certainty that Khandekar designed the scripts to circumvent KCG's security protocols, which would have blocked him from directly accessing the information from the SVN.

### 2. Khandekar engaged in unauthorized access and breached KCG security.

I have also concluded, based on my review of the evidence above, that Khandekar's access of confidential source code information constitutes a security breach and unauthorized access under KCG policies. Specifically, Section 3.3.1 of KCG's Acceptable Use Policy prohibited KCG employees from "…accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access."

[9] The process scripts filtered out specific code file names of non-confidential code files, including, but not limited to the following: [redacted] (KCG010656).

Khandekar has asserted that he was authorized to access the confidential source code files in other users' directories because he was able to open and read the files. At his deposition, for example, he testified that, "[redacted], by setting explicit read and access permissions for the files in their directories as well as all the directories enclosing those files, gave me an authorization and permission to access those files." Khandekar Tr. at 174.

Based on my 25+ years of experience in data security, a policy that requires an employee to obtain "express authorization" for access to confidential information requires some affirmative act granting permission; it cannot be satisfied by the mere absence of encryption or the placing of a file in a folder with read/write access. The factual context in this case confirms that Khandekar lacked even *implied* authorization, let alone express authorization. Khandekar has admitted that he did not have express written or verbal permission from the authors of the source code files and that he was aware that he was not permitted to have knowledge of other employees' confidential source codes. Further, each of the [redacted] source code files at issue contained a list of authorized users (*i.e.,* the Additional PGP Recipients), which did not include Khandekar. Thus, it is my professional opinion that Khandekar lacked the requisite authorization to access the source code files and breached KCG security by accessing, copying and reviewing those files.

## VI. Summary of Timeline Events

I have found the events set forth below to have occurred between December 28, 2016 and March 28, 2017. Further detail, including the full Bash Command History, is attached as **Exhibit C**.

**December 28, 2016:** Khandekar runs a Scan Script to search for [redacted] source code files on the build server in other users' directories, views the content of the SVN source code repository ("src"), copies all files present in the src repository into his own directory, and reads those files. Khandekar then runs a second Scan Script to identify source code files and then runs a Process Script to filter out certain types of sample and test source code files.

**December 29, 2016:** Khandekar views the content of a third Scan Script folder, reads specific source code files in folders he created in his own directory to mimic [redacted] directory, lists and copies all of [redacted]s files in the SVN src into his own directory, runs a Process Script to filter out certain source codes, copies source code files from [redacted] and [redacted] directories to his own, reads source code files, and deletes certain files and subfolders from his directory. Khandekar then copies all source code files from [redacted] directory to his own, and re-runs Process Scripts to filter out certain source code files.

**December 30, 2016:** Khandekar copies files from [redacted] directory, re-runs a Process Script and views the contents of Process Script output files, which list source codes copied from other users' directories.

**January 2 - 3, 2017:** Khandekar views and filters source code files copied from other users' directories.

**January 9 – 15, 2017:** Khandekar views source code files copied from other users' directories.

**January 21, 2017:** Khandekar views source code files copied from other users' directories.

**January 23, 2017:** Khandekar views source code files copied from other users' directories.

**January 25, 27, 2017:** Khandekar views source code files copied from other users' directories and lists contents of directories he created in his own directory of source code files.

**January 28, 2017:** Khandekar views source code files copied from other users' directories, runs a comparison of two source code files copied from other users' directories, creates a new folder called "done," and moves certain source code files to the "done" folder.

**January 30, 2017:** Khandekar runs comparisons of source code files copied from other users' directories, read source code files, and moves source code files to the "done" folder.

**February 2, 2017:** Khandekar moves source code files copied from other users' directories into the "done" folder.

**February 3, 2017:** Khandekar reads source code files copied from other users' directories.

**February 5, 2017:** Khandekar reads source code files copied from other users' directories and moves certain source code files to the "done" folder.

**February 6, 2017:** Khandekar moves source code file to the "done" folder.

**February 7, 2017:** Khandekar reads source code files copied from [redacted] directory.

**February 10, 2017:** Khandekar copies source code files from the SVN src folder in [redacted] directory to his own directory.

**February 12, 2017:** Khandekar opens source code files copied from [redacted] user directory.

**February 16, 2017:** Khandekar opens and reads source code files and source code header files copied from other users' directories.

**February 21, 2017:** Khandekar opens source code files copied from other users' directories.

**February 22, 2017:** Khandekar copies and reads source code files, and deletes certain source code files.

**February 24, 2017:** Khandekar clones an entire git folder in [redacted] directory, saves it to a folder he created on his own directory, and renames folder holding source code files he obtained from other users to a hidden ".bs" folder.

**February 26, 2017:** Khandekar opens source code files copied from [redacted] and [redacted] directories.

**March 6, 2017:** Khandekar deletes folders with source code files and his entire .bs directory.

**March 14, 2017:** Khandekar gives notice of resignation to KCG.

**March 16, 2017:** Khandekar deletes his Evernote directory.

**March 20, 2017:** Khandekar wipes his personal Samsung phone, which he also uses for business purposes, using the factory reset function.

**March 21, 2017:** Khandekar deletes the content of a directory named "take_home" and deletes a .zip file.

**March 28, 2017:** Khandekar deletes his entire docs directory.

**March 30, 2017:** Khandekar's last day at KCG; turns in his KCG-issued laptop wiped.

## VII. Summary of Conclusions

Based on my review and analysis of the evidence described above, I have drawn the following opinions and conclusions:

**A.** Khandekar breached KCG security and violated KCG policies that restricted him from accessing confidential information without authorization.

**B.** Khandekar executed various operations designed to circumvent KCG's data security policies and procedures in order to access and copy confidential source code and Predictors developed by other Quantitative Strategists.

**C.** Khandekar developed and used the Khandekar Scripts to search other users' folders and directories for [redacted] files.

**D.** Between December 28, 2016 and March 28, 2017, Khandekar ran the scripts he created on multiple occasions against other users' folders and directories and performed numerous operations in other users' folders and directories, such as viewing, copying and filtering files.

**E.** Khandekar obtained [redacted] confidential source code files developed by other users.

**F.** Khandekar took explicit steps to hide and destroy evidence that he accessed, copied or viewed confidential source code files that he obtained from other users' directories.

**Very truly yours,**

**Bruce V. Hartley, CISSP**

# EXHIBIT A - Curriculum Vitae of Dr. Bruce V. Hartley, CISSP

# Curriculum Vitae of Dr. Bruce V. Hartley, CISSP

322 Grand Overlook Drive, Seneca, SC 29678 | (719) 651-6651 (direct) | bhartley@areteadvisorsinc.com

## SUMMARY:

Dr. Hartley has held numerous executive management and C-level positions in venture-backed, privately held, and public technology firms. Experience includes creating and managing rapid growth technology organizations that create leading edge products and services to the cyber security and digital forensics industries. Dr. Hartley holds two technology patents, one in the software architecture space and the other in the cyber security space.

Dr. Hartley is currently the Chief Operating Officer at Arete Advisors, Inc. Arete Advisors is a Cyber Security firm that focuses on data-centric investigations. Prior to Arete he was the Chief Technology Officer at Discovia. Prior to Discovia, Bruce was Vice President of the Celerity Consulting Group, where he led the Digital Forensics and Investigations practice. Prior to Celerity, he was the National Director for Discovery Services at Deloitte FAS, LLP. Before joining Deloitte, he was the Chief Technology Officer at Cricket Technologies and the IT Sector Director at bd Systems, Inc. (now part of SAIC).

Dr. Hartley brings extensive experience across the entire cyber security, digital forensics, and electronic discovery spectrums. He has experience as an expert witness in support of multiple litigations involving such issues as electronic mail fraud, software development process and contracts, data destruction, intellectual property disputes (software/source code theft), protection of company confidential and proprietary information, and trade secret misappropriation.

Dr. Hartley has been a presenter, panel speaker, instructor, and round table representative at several industry conferences and seminars. Also, Dr. Hartley has authored numerous publications on information security, computer forensics, electronic discovery, records management and other related topics.

Recognized by the National Computer Security Center as a Vendor Security Analyst and certified by the ISC$^2$ as a Certified Information System Security Professional (CISSP), Certification No. 4140.

## EDUCATION

- Doctorate in Computer Science - Colorado Technical University, Colorado Springs, CO
- Master of Arts in Computer Data Management - Webster University, St. Louis, MO, Distinguished Graduate
- Bachelor of Science in Technical Management and Computer Science – Regis College, Denver, CO, Dean's Honor Roll

## PATENTS

- *Method and Apparatus for Assessing the Security of a Computer System.* Patent awarded May 3, 2005, Patent number 6,889,168.
- *Operational System for Operating on Client Defined Rules.* Patent awarded March 11, 2003, Patent number 6,532,465.

## PROFESSIONAL EXPERIENCE

**Arete Advisors, Inc. – Chief Operating Officer, Greenville, SC**
**October 2017 – Present**

Bruce joined Arete Advisors in October 2017 as the Chief Operating Officer where he is responsible for the delivery of high-quality cyber, incident response, digital forensics, and expert witness services across the company.

**Discovia – Chief Technology Officer, Greenville, SC and San Francisco, CA**
**January 2016 – September 2017**

As the Chief Technology Officer, Bruce was responsible for the information technology infrastructure, security, development, and support at Discovia. He directed and managed the application development teams in the US and India as well as the IT Support Team in San Francisco, CA. Successfully migrated email from on premise MS Exchange to Office 365 in the Microsoft cloud, replaced the on-site PBX system and implemented Skype for Business, and completed a major infrastructure upgrade to the internal hosting and review environment. He prepared for and passed independent third-party security audits leading to both ISO 27001 and HPAA security certifications.

In addition, Bruce consulted with corporate clients to solve complex problems related to the collection and analysis of extremely large data sets (big data) and provides expert analysis and testimony as required.

He offered expertise across the entire litigation lifecycle, leading teams in support of large FCPA investigations, class action lawsuits, SEC investigations, HSR Second Requests, DOJ investigations, and assisting clients with the integration of discovery-related technologies.

He also provided expert witness services in support of multiple litigations involving such issues as electronic mail fraud, software copying/theft, software development process and contracts, data destruction, and intellectual property disputes.

**Discovia – Vice President, Greenville, SC and San Francisco, CA**
**May 2015 – December 2015**

Bruce joined Discovia as Vice President in May 2015 to co-lead the Digital Forensics and Analytics practice. In this capacity he led teams performing forensic data collections and analysis, incident and breach response, and provided expert witness services for trade secret and intellectual property (software) theft cases.

**Celerity Consulting Group – Vice President, Denver, CO and San Francisco, CA**
**October 2012 – May 2015**

Lead the Litigation Technology Integration Practice assisting clients in deploying and leveraging complex e-discovery tools and technologies, such as those developed by HP, Symantec, Access Data, etc. in support of large complex litigations and investigations. Manages the e-discovery practice assisting clients in responding to litigations, investigations, etc. Services include computer forensics, discovery processing, hosting, and review. Also provides Expert and Fact Witness services on e-discovery and intellectual property related matters.

**Compute Intensive, Inc. – President and CEO, Denver, CO**
**June 2011 – October 2012**

Provideed expert technology consultation and support services in the areas of litigation support, information security, and network engineering. Led numerous Autonomy-related integration and implementation efforts supporting the entire EDRM process. Functions as an Expert Witness on technology-related matters such as IP theft, fraud, and contract disputes.

**Deloitte Financial Advisory Services, LLP. – National Director, Electronic Discovery Subject Matter Expert, Denver, CO and Hermitage, TN**
**June 2010 – February 2012**

Functioned as a national e-discovery subject matter expert for Deloitte FAS' Discovery service line. Led FAS' implementation of their legal holds management system, remote desktop collection system, early case assessment capability, electronic discovery processing system and our next generation review and production platform using Autonomy's IDOL v7 technology. Recently led the implementations of an enterprise-wide remote data collection, early case assessment, and e-discovery processing systems using both Access Data and HP Autonomy technologies for multiple clients.

Manage the technical team in Hyderabad, India that provides computer forensic and electronic discovery services to the US Practice.

Frequently engaged as an Expert Witness on e-discovery process and/or technology oriented matters, such as intellectual property disputes. Served as the Deloitte FAS representative to the US Deloitte LLP Technology Advisory Council to help define and drive technology solutions across the Deloitte US companies.

**Deloitte Financial Advisory Services, LLP. – National Director, Electronic Discovery**
**Washington, DC and Hermitage, TN**
**October 2005 – June 2010**

Functioned as a National E-Discovery Subject Matter Expert (SME) for Deloitte FAS' Discovery service line. Led FAS' implementation of their legal holds management system, remote desktop collection system, early case assessment capability, electronic discovery processing system and their next generation review and production platform. Led the implementations of an enterprise-wide remote data collection, early case assessment, and e-discovery processing systems using both Access Data and HP Autonomy technologies for multiple clients.

Managed the technical team in Hyderabad, India that provides computer forensic and electronic discovery services to the US Practice (follow-the-sun model).

Served as the Deloitte FAS representative to the Deloitte LLP Technology Advisory Council to help define and drive technology solutions across the Deloitte US companies.

Led the design and development of Deloitte's Electronic Discovery Solutions Center (EDSC) deploying over 1,000 physical servers with 5 petabytes of dedicated storage. At the time of deployment, the EDSC was the most advanced data center in the Deloitte US Company, designed to meet key Tier III and Tier IV data center requirements.

**Cricket Technologies, LLC. – Chief Technology Officer**
**Reston, VA**
**July 2004 – September 2005**

Was a member of the executive management team responsible for all software development efforts, computer forensics services, electronic discovery operations, paper (scan and OCR) production, and network operations. Provided technical direction, oversight, and vision for future technologies, products, and services. Led the re-design and development efforts for the Cricket e-discovery appliance which was designed specifically for the litigation support market.

**bd Systems, Inc. – IT Sector Director**
**Colorado Springs, CO**
**December 2002 – July 2004**

Responsible for managing and directing approximately 130 people including organizations located in Colorado Springs, CO, San Antonio, TX, Washington D.C., Oakland, Los Angeles and Pasadena, CA. The IT Sector provided network engineering and enterprise management as well as information protection/assurance services to Air Force Space Command, intelligence analyst support, and custom software development to the Air Intelligence Agency, and specialized technical support to NASA.

**Privisec, Inc. – Founder, President, and Chief Executive Officer**
**Colorado Springs, CO**
**April 2002 – October 2005**

Founded Privisec, Inc. to provide top quality cyber security and forensic consulting services to the financial, healthcare, and local and state Government communities. Frequently lead hands-on security assessment and penetration tests and was routinely invited to speak at industry conferences in both the Financial and Government sectors. Often interviewed and quoted by the press on cyber security related matters.

**PoliVec, Inc. – Founder, President and Chief Executive Officer**
**Colorado Springs, CO**
**October 1999 – April 2002**

As the founder of the company, was responsible for the overall direction and operation of PoliVec, Inc. This included leading the effort to obtain $9 million in funding from a Silicon Valley venture capital firm to establish the company as a key player in the enterprise information security arena for both products and services.

During my tenure as CEO, the company grew from the 3 original founders to approximately 40 employees. Within its first 18 months, developed and shipped the PoliVec Builder and PoliVec Scanner products, gained significant early traction with over 30 customers, and received favorable product reviews and awards from such publications as InfoWorld and SC magazine.

**DMW Worldwide - Executive Vice President and Chief Operating Officer**
**Colorado Springs, CO**
**February 1998 - February 2000**

While at DMW, re-directed the company's operational entities and product development focus of the Entero Customer Care and Billing product to address the IP-centric market. Accomplishments included delivering the Entero Commissions product to several Competitive Local Exchange Carriers (CLECs), and directing the HostCHECK Unix security software development effort DMW was successfully sold to Mindport, a provider of software products and support services for traditional and broadband distributors of pay media.

**DMW Worldwide Senior Vice President and Chief Technology Officer**
**Colorado Springs, CO**
**January 1997 - February 1998**

As the SVP of Professional Services, was responsible for the creation, development, and operation of the Network Engineering and Information Protection Consulting practice. The practice focused on providing high-profile commercial clients, such Time-Warner, Qwest Communications, McGraw-Hill, AIG Insurance, SGI, and AT&T Capital, with enterprise-wide cyber security services and the development of automated security tools to enhance a client's ability to maintain a consistent security posture.

As the Chief Technology Officer, directed the re-design and re-engineering effort of the Entero product using objected-oriented technology, defined and implemented new software development processes, and created a software test and quality assurance organization. Successfully deployed the first release of the Entero Customer-Care and Billing system to the first cellular reseller in Japan.

**Trident Data Systems - Senior Vice President and Chief Technology Officer**
**Los Angeles, CA**
**July 1995 – December 1996**

One of five key executives who managed this 1,100-person company with over a dozen physical locations and over $100M in annual revenue. Provided overall strategic technical direction and planning for all operational locations throughout the United States. In addition, completed numerous company initiatives including the creation of regional laboratories for cyber security, rapid applications development, document imaging, and Local Area Network/Wide Area Network technologies.

**Trident Data Systems - Vice President of Technology and Chief Information Officer**
**Colorado Springs, CO and Los Angeles, CA**
**July 1994 - July 1995**

As the CIO, led the development of a custom Oracle-based Human Resources system, implemented an enterprise Internet firewall system based on Checkpoint-1, upgraded the corporate electronics mail system from a Macintosh-based solution to an enterprise mail solution using MS Exchange, and upgraded the accounting system from an aging Oracle Financials solution running on HP-UX to a Deltek-based solution running on Solaris.

**Trident Data Systems - Director, Colorado Springs Operations**
**Colorado Springs, CO**
**February 1991 - July 1994**

Responsible for all Colorado Springs, CO operations and grew the office from 5 employees to over 80 in this period with an increase in annual revenues from less than $500,000 to over $10M. Program Manager and Technical Lead on the Consolidated Space Operations Center Integration and Activation Support Contract. During tenure as Program Manager, we received three consecutive 100% award fees. Was the Proposal Manager and Technical Volume Lead on the successful Government proposal effort, leading to a 5 year $50M contract with HQ Air Force Space Command.

**Unisys Defense Systems - Project Manager**
**Colorado Springs, CO**
**January 1990 - February 1991**

Responsible for operating and maintaining the Air Force Space Command Mission Support Netwok with nodes at Falcon Air Force Base, CO, Onizuka Air Force Base, CA, and Los Angeles Air Force Base, CA. Managed a technical staff of 22 and provided communications and security engineering support.

**Arca Systems - Chief Engineer**
**San Jose, CA**
**May 1988 - December 1989**

Responsible for the technical direction and excellence of all Arca Systems projects. Program Manager and Technical Lead on the ARGUS multi-level secure database development effort, which was the first implementation of the integrity lock concept outside of academia. Developed the Informal Security Policy Model, the Detailed Top-Level Specification and Security Test Plans and Procedures for a B1 level system in accordance with DoD 5200.28-Std (Orange Book). Developed and instructed the Arca Computer Security and Arca Network Security courses delivered to numerous commercial and Government organizations.

**Computer Technology Associates (CTA) - Senior Engineer**
**Colorado Springs, CO**
**January 1985 - May 1988**

Project Manager and Technical Lead for the United States Space Command Space Command Center Integration effort, the World Wide Military Command and Control System Information System installation in the NORAD Cheyenne Mountain Complex, and the WWMCCS Host installation at Cheyenne Mountain.

### Other Related Experience

Developed and taught numerous computer science courses at multiple colleges and universities since 1985. Previously an Adjunct Professor of Computer Sciences and a member of the Technical Advisory Board at Colorado Technical University, Colorado Springs, CO focusing on the design and development of their cyber security degree programs.

Published over 25 articles and technical papers in such publications as Internet Security Advisor, Data Communications, Information Security, DM Review, COTS Journal, Lotus Advisor, and the Metropolitan Corporate Counsel.

## INVITED TALKS, PRESENTATIONS, AND RELATED ACTIVITES

Presented at numerous conferences in the United States, Canada, and Europe on numerous information technology and security related topics. These conferences include Legal Tech New York, Network World + Interop, Communications Networks (ComNet), Sun World, Federal Information Superiority Conference (FISC), Vanguard Enterprise Security Expo, NAFCU Annual Conference and Expo, NAFCU Security Workshop, The Legal and Strategic Guide to Electronic Discovery, IQPC Records Management and e-Discovery Conference, the International CERT Conference, Techno Security and Mobile Forensics, and the Northern California e-Discovery Retreat. Also developed and presented CLE sessions on computer forensics and electronic discovery for Sidley Austin, LLP., Jones Day University, and Mayer Brown University in Chicago, Los Angeles, CA, Washington DC, and New York, NY.

## EXPERT WITNESS AND TESTIMONY EXPERIENCE

*Syinverse Technologies, Inc., -v BellSouth Telecommunications, Inc.*
Florida Middle District Court
Case No. 8:2005cv00777
Designated by Plaintiff as Testifying Computer Software Expert

*Illinois State Board of Investment –v Amerigroup Corporation, et al*
United States District Court, Eastern District of Virginia
Case No. 2:05-CV-701 (HCM-FBS)
Designated by Defendants as Testifying Computer Forensics Expert

*Citadel Investment Group, LLC., et al –v Mikhail Malyshev, et al*
American Arbitration Association
Case No. 51 166 00969 09 and 51 166 00970 09
Designated by Defendants as Testifying Computer Software and Computer Forensics Expert

*Department of Navy, Office of Naval Research –v 21st Century Systems, Inc.*
Armed Services Board of Contract Appeals (ASBCA), Contract No. N00014-11-Q-0015
Case No. ASBCA 56213

Designated by Plaintiff as Testifying Computer Software Expert

*MoneyGram Payment Systems, Inc., -v RBD Securities, Inc.*
State of Minnesota District Court, Fourth Judicial District
Case No. 27-cv-12-1349
Designated by Plaintiff as Testifying Electronic Discovery Expert

*Brady –v Reyes*
Superior Court of California, County of Santa Clara
Case No. 6-10-FL-003968
Designated by Defendants as Electronic Discovery Expert

*Move, Inc. et al –v Zillow, Inc., et al*
Superior Court of Washington for King County
Case No. 14-2-07669-0 SEA
Designated by Defendants as Testifying Computer Forensics Expert

*Bartech Systems International, Inc., -v Mobile Simple Solutions, Inc., et al*
Eighth Judicial District Court
Case No. A-14711544-B
Designated by Defendants as Testifying Computer Software and Computer Forensics Expert

*Waymo LLC. –v Uber Technologies, Inc., et al*
United States District Court, Northern District of California, San Francisco Division
Case No. 3:17-cv-00939-WHA (Case On-Going)
Designated by Plaintiffs as Testifying Computer Security Expert

*KCG Holdings, Inc. –v Rohit Khanderkar*
United States District Court, Sothern District of New York
Case No. 17 CV 3533 (Case On-Going)
Designated by Plaintiffs as Testifying Computer Software and Security Expert

**RELEVANT PUBLICATIONS**

- *Get the Jump on E-Forensics*, The Metropolitan Corporate Council, 2005
- *Financial Institution Security – Case Studies*, Credit Union Tech-Talk, 2002
- *Developing Effective Security Policies*, Lotus Advisor Magazine, 2001
- *Safer E-Commerce*, Business Security Advisor, 2001
- *Windows NT or Linux: Which is More Secure?*, Business Security Advisor, 2001.
- *Security as a Process*, with Anthony D. Locke, DM Review, 2001
- *Why is Computer Crime on the Rise?*, Business Security Advisor, 2001
- *Improve Host Security*, Business Security Advisor, 2001
- *Denial of Service…or Just Denial?*, Internet Security Advisor, 2001

- *Policy-Driven Network Security: A Proactive Approach to Securing the Enterprise*, COTS Journal, 2000
- *ASP Security: Who is Watching Your Business' Future*, Internet Industry Magazine, 2000
- *A Proactive Approach to Securing the Enterprise*, Internet Security Advisor, 2000
- *ILOVEYOU: Another Good Reason to Re-Visit Corporate Security Practices*, Internet Security Advisor, 2000
- *Honey-Pots: A New Dimension to Intrusion Detection*, Internet Security Advisor, 2000
- *Today, More Than Ever, We Must Think About Security*, Internet Security Advisor, 2000
- *Is Your Network Inviting Attack*, with Eric Knight, Internet Security Advisor, 2000
- *Policy-Based Security for e-Business*, Internet Security Advisor, 2000
- *Anatomy of a Vulnerability*, Internet Security Advisor, 2000
- *Move to e-Business with Confidence*, Internet Security Advisor, 1999
- *Get Your Network Ready for e-Business*, Security Advisor, 1998
- *Test of Strength and Security*, Information Security, 1998
- *You Need a Corporate Security Policy*, Security Advisor, 1998
- *The Password Paradox: Insecure Security*, Internet Security Advisor, 1998
- *Ensure the Security of Your Corporate Systems*, Security Advisor, 1998
- *Securing e-Commerce Without Heavy Investment*, Data Communications, 1998
- *Virtual Private Networks*, Internet Security Advisor, 1998
- *Data Security for Medical Information Systems and Confidentiality and Privacy Protection*, Auerbach Publishing,
  New York, 1996
- *Ensuring Data Confidentiality and Integrity in Medical Information Systems: Defining a Security Policy*, Thompson Publishing Group, New York, 1995

## EXHIBIT B – KHANDEKAR SCRIPTS

**Scan.sh**

| Command Syntax | Actions Performed |
|---|---|

[redacted]

**Scan.sh (continued)**

| Command Syntax | Actions Performed |
|---|---|

[redacted]

**Process.sh**

Actions Performed

[redacted]

## Scan2.sh

### Actions Performed

[redacted]

## Process2.sh

### Actions Performed

[redacted]

## Scan3.sh

Actions Performed

[redacted]

## Process3.sh

### Actions Performed

[redacted]

**Scan3a.sh**

[redacted]

EXHIBIT C – BASH HISTORY

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]